



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/505,175	08/31/2004	Satoshi Kitani	255635US6PCT	8272
22850 7590 08/09/2007 OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C. 1940 DUKE STREET ALEXANDRIA, VA 22314			EXAMINER MEDE, ESTEVE	
			ART UNIT 2137	PAPER NUMBER
			NOTIFICATION DATE 08/09/2007	DELIVERY MODE ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	Application No. 10/505,175	Applicant(s) KITANI ET AL.	
	Examiner Esteve Mede	Art Unit 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 31 August 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-25 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-25 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>08/31/2004</u> . | 6) <input type="checkbox"/> Other: _____ |

Specification

1. The disclosure is objected to because of the following informalities: The applicant failed to layout the specification according to 37 CFR 1.177(b) guidelines (see below for correct layout of the specification).

The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

- (a) TITLE OF THE INVENTION.
- (b) CROSS-REFERENCE TO RELATED APPLICATIONS.
- (c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
- (d) THE NAMES OF THE PARTIES TO A JOINT RESEARCH AGREEMENT.
- (e) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC.
- (f) BACKGROUND OF THE INVENTION.
 - (1) Field of the Invention.
 - (2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
- (g) BRIEF SUMMARY OF THE INVENTION.
- (h) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
- (i) DETAILED DESCRIPTION OF THE INVENTION.
- (j) CLAIM OR CLAIMS (commencing on a separate sheet).
- (k) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
- (l) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

The specification does not provide for the section heading as described above.

Appropriate correction is required.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim 4 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 4 discloses a program of a reproducing apparatus and an information processing apparatus for recording information to a recording medium. For the claim to be statutory the program must be implemented in a computer readable medium (storage). The claim as read can be considered by one of ordinary skill in the art as software per se, and therefore does not appear to be implemented in a computer readable medium (storage).

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-10, and 24-25 are rejected under 35 U.S.C. 102(e) as being anticipated by Kamibayashi et al. (US 7,065,648).

Regarding claims 1, 4, 5, 24, Kamibayashi discloses a mutually authenticating method for mutually authenticating a reproducing apparatus and an information processing apparatus, the reproducing apparatus comprising a reproducing portion for reading content information from a recording medium having revocation information and information unique to the recording medium, the revocation information being used to determine whether or not an electronic device is illegal, the reproducing apparatus being configured to transmit and receive the content information to and from the information processing apparatus for processing the content information (see abstract col. 8, lines 47-67; column 9, lines 1-65), the mutually authenticating method comprising the steps of: causing the reproducing apparatus to determine whether or not the reproducing apparatus itself should be invalidated using information that represents the reproducing apparatus and the revocation information (see abstract col. 8, lines 47-67; column 9, lines 1-65); causing the information processing apparatus to determine whether or not the information processing apparatus itself should be invalidated using the information that represents the information processing apparatus and the revocation information; and causing the reproducing apparatus and the information processing apparatus to mutually authenticate each other using both first key information generated when the determined result at the first determining step does not represent that the reproducing apparatus should be invalidated and second key information generated when the determined result at the second determining step does not represent that information processing apparatus should be invalidated (see abstract col. 8, lines 47-67; column 9, lines 1-65).

Regarding claim 2, Kamibayashi discloses the mutually authenticating, wherein the mutually authenticating step comprises the steps of: causing the reproducing apparatus to confirm whether or not the information processing apparatus normally operates through the transferring means; and causing the information processing apparatus to confirm whether or not the reproducing apparatus normally operates through the transferring means (col. 8, lines 47-67; column 9, lines 1-65).

Regarding claims 3, and 8, Kamibayashi discloses the mutually authenticating method as set forth in claim 2, further comprising the steps of: causing the reproducing apparatus to generate a random number (col. 8, lines 47-67; column 9, lines 1-65); causing the reproducing apparatus to perform a predetermined calculation (col. 8, lines 47-67; column 9, lines 1-65); causing the information processing apparatus to generate a random number (col. 8, lines 47-67; column 9, lines 1-65); and causing the information processing apparatus to perform a predetermined calculation (col. 8, lines 47-67; column 9, lines 1-65), wherein the first confirming step comprises the steps of: causing the reproducing apparatus and the information processing apparatus to mutually exchange a first random number generated at the first random number generating step with a second random number generated at the second random number generating step (col. 8, lines 47-67; column 9, lines 1-65); and causing the reproducing apparatus to compare the result calculated at the first calculating step using at least the first key information, the first random number, and the second random number, the first random number and the second random number having been mutually exchanged, with the result calculated at the second calculating step using at

least the second key information, the first random number, and the second random number, the second key information, the first random number, and the second random number having been transmitted from the information processing apparatus through the transferring means, the first random number and the second random number having been mutually exchanged, and wherein the second confirming step comprises the steps of (col. 8, lines 47-67; column 9, lines 1-65); causing the reproducing apparatus and the information processing apparatus to mutually exchange a third random number generated at the first random number generating step with a fourth random number generated at the second random number generating step (col. 8, lines 47-67; column 9, lines 1-65); and causing the information processing apparatus to compare the result calculated at the first calculating step using at least the first key information, the third random number, and the fourth random number, the first key information, the third random number, and the fourth random number having been transmitted from the reproducing apparatus through the transferring means, the third random number and the fourth random number having been mutually exchanged, with the result calculated at the second calculating step using at least the second key information, the third random number, and the fourth random number, the third random number and the fourth random number having been mutually exchanged (col. 8, lines 47-67; column 9, lines 1-65).

Regarding claims 6 and 25, Kamibayashi discloses a signal processing system comprising a reproducing apparatus and an information processing apparatus, the reproducing apparatus comprising a reproducing portion for reading content

information from a recording medium having revocation information and information unique to the recording medium, the revocation information being used to determine whether or not an electronic device is illegal, the reproducing apparatus being configured to transmit and receive the content information to and from the information processing apparatus for processing the content information (col. 8, lines 47-67; column 9, lines 1-65), wherein the reproducing apparatus further comprises: first determining means for determining whether or not the reproducing apparatus itself should be invalidated using information that represents the reproducing apparatus and the revocation information (col. 8, lines 47-67; column 9, lines 1-65), wherein the information processing apparatus comprises : second determining means for determining whether or not the information processing apparatus itself should be invalidated using the information that represents the information processing apparatus and the revocation information (col. 8, lines 47-67; column 9, lines 1-65), and wherein the signal processing system further comprises: mutually authenticating means for causing the reproducing apparatus and the information processing apparatus to mutually authenticate each other using both first key information generated when the determined result of the first determining means does not represent that the reproducing apparatus should be invalidated and second key information generated when the determined result of the second determining means does not represent that information processing apparatus should be invalidated (col. 8, lines 47-67; column 9, lines 1-65); and common key generating means for generating a common key that is in common with the reproducing apparatus and the information processing apparatus

after the mutually authenticating means has mutually authenticated the reproducing apparatus and the information processing apparatus (col. 6, lines 61-67; column 7, lines 1-11).

Regarding claim 7, Kamibayashi discloses the signal processing system as set forth in claim 6, wherein the mutually authenticating means comprises: first confirming means for confirming whether or not the information processing apparatus normally operates through the transferring means; and second confirming means for confirming whether or not the reproducing apparatus normally operates through the transferring means (see figure 1, of the drawings; col. 6, lines 30-36).

Regarding claim 9, Kamibayashi discloses the signal processing system as set forth in claim 8, wherein the common key generating means comprises: third random number exchanging means for mutually exchanging a fifth random number generated by the first random number generating means with a sixth random number generated by the second random number generating means between the reproducing apparatus and the information processing apparatus (col. 8, lines 47-67; column 9, lines 1-65); first common key generating means for generating the common key for the reproducing apparatus using at least the first key information, the fifth random number, and the sixth random number; and second common key generating means for generating the common key for the information processing apparatus using at least the second key information, the fifth random number, and the sixth random number (see figure 1, of the drawings; col. 6, lines 30-36, col. 7, lines 20-28).

Regarding claim 10, Kamibayashi discloses the signal processing system as set forth in claim 9, further comprising: first transmitting means for transmitting information from the reproducing apparatus to the information processing apparatus through the transferring means in accordance with a common key encrypting system using the common key (see figure 1, of the drawings; col. 6, lines 30-36, col. 7, lines 20-28), wherein the reproducing apparatus further comprises; intermediate key information generating means for generating key information unique to the recording medium using the first key information and the information unique to the recording medium (col. 2, lines 44-48).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 11-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kamibayashi et al. (US 7,065,648 B1) in view of Tagawa et al. (US 6,615,192 B1).

Regarding claim 11, Kamibayashi discloses all the limitations of claim 11 except for the signal processing system as set forth in claim 10, further comprising: key information encrypting means for encrypting third key information using at least the key information unique to the recording medium; encryption key information recording means for recording the third key information encrypted by the key information encrypting means to the recording medium; final encryption key generating means for

generating a content information encryption key in accordance with the third key information; and content information recording means for recording content information encrypted using the content information encryption key to the recording medium.

Tagawa discloses a key information encrypting means for encrypting third key information using at least the key information unique to the recording medium; encryption key information recording means for recording the third key information encrypted by the key information encrypting means to the recording medium; final encryption key generating means for generating a content information encryption key in accordance with the third key information. According to CPRM a "final key" is the "title key". And content information recording means for recording content information encrypted using the content information encryption key to the recording medium (col. 1, lines 29-48).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Kamibayashi to include the used of encryption title key (i.e. third key information) in order to encrypt content into a recordable media in encrypted form, such that the content may be secure from unauthorized third parties.

Regarding claim 12, Tagawa the signal processing system as set forth in claim 11, wherein the information processing apparatus comprises the key information encrypting means, the encryption key information recording means, the final encryption key generating means, and the content information recording means, and wherein the first transmitting means is configured to transmit the key information unique to the

recording medium to the information processing apparatus (col. 1, lines 29-48; lines 60-67; col. 2, lines 1-16).

6. Claims 13-14 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kamibayashi et al (US 7,065,648 B1) in view of Tagawa et al. (US 6,615,192 B1) further in view of (US 6,640,137 B1).

Regarding claim 13, Kamibayashi and Tagawa discloses all the limitations of claim 13, except for, wherein the third key information is key information in accordance with a seventh random number generated by the first random number generating means of the reproducing apparatus.

Akiyama discloses a title key (third key information) is key information in accordance with a random number generator (see abstract). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Kamibayashi in order to create a unique title key for the recording media, such that each title key created maybe different from each other.

Regarding claim 14, Akiyama discloses the signal processing system as set forth in claim 12, wherein the third key information is key information in accordance with an eighth random number generated by the second random number generating means of the information processing apparatus (see abstract).

Regarding claim 15, Tagawa discloses the signal processing system as set forth in claim 11, wherein the information processing apparatus comprises the key information encrypting means, the encryption key information recording means, and

the content information recording means, wherein the first transmitting means is configured to transmit the key information unique to the recording medium to the information processing apparatus, wherein the reproducing apparatus comprises the final encryption key generating means, wherein the first transmitting means is configured to transmit the content information encryption key generated by the final encryption key generating means to the information processing apparatus (col. 1, lines 29-48; lines 60-67; col. 2, lines 1-16).

Regarding claim 16, Akiyama discloses the signal processing system as set forth in claim 15, wherein the third key information is key information in accordance with a ninth random number generated by the first random number generating means of the reproducing apparatus (see abstract).

Regarding claim 17, Tagawa discloses the signal processing system wherein the third Key information is key information in accordance with a tenth random number generated by the second random number generating means of the information processing apparatus, and wherein the signal processing system further comprises: second transmitting means for transmitting information from the information processing apparatus to the final encryption key generating means of the reproducing apparatus through the transferring means in accordance with the common key encrypting system using the common key (col. 1, lines 29-48; lines 60-67; col. 2, lines 1-16).

Regarding claim 18, Tagawa discloses the signal processing apparatus, further comprising: key information decrypting means for decrypting fourth key information that has been encrypted and read from the recording medium using at least the key

information unique to the recording medium; final decryption key generating means for generating content information decryption key in accordance with the fourth key information; and content information decrypting means for decrypting the content information using the content information decryption key (col. 1, lines 29-48; lines 60-67; col. 2, lines 1-16).

Regarding claim 19, Tagawa discloses the signal processing system as set forth in claim 18, wherein the information processing apparatus comprises the final decryption key generating means and the content information decrypting means (col. 1, lines 29-48; lines 60-67; col. 2, lines 1-16).

Regarding claim 20, Tagawa discloses the signal processing system as set forth in claim 19, wherein the information processing apparatus comprises the key information decrypting means, and wherein the first transmitting means is configured to transmit the key information unique to the recording medium to the information processing apparatus (col. 1, lines 29-48; lines 60-67; col. 2, lines 1-16).

Regarding claim 21, Tagawa discloses the signal processing system as set forth in claim 19, wherein the reproducing apparatus comprises the key information decrypting means, and wherein the first transmitting means is configured to transmit the decrypted fourth key information to the information processing apparatus (col. 1, lines 29-48; lines 60-67; col. 2, lines 1-16).

Regarding claim 22, Tagawa discloses the signal processing system as set forth in claim 18, wherein the reproducing apparatus comprises the final decryption key generating means (col. 1, lines 29-48; lines 60-67; col. 2, lines 1-16).

Regarding claim 23, Tagawa discloses the signal processing system as set forth in claim 22, wherein the reproducing apparatus comprises the key information decrypting means, and wherein the first transmitting means is configured to transmit the content information decryption key generated by the reproducing apparatus to the information processing apparatus (col. 1, lines 29-48; lines 60-67; col. 2, lines 1-16).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Esteve Mede whose telephone number is 571-270-1594. The examiner can normally be reached on Monday thru Friday, 8:30-5:00 PM, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2137

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Esteve Mede

EM

August 3, 2007


EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER